SaTC: STARSS: Small: Collaborative: Managing Hardware Security in Three Dimensional Integrated Circuits

Qiaoyan Yu, University of New Hampshire

https://mypages.unh.edu/qyu/research

Introduction

- 3D IC comes with new security challenges
- New types of hardware Trojans can be launched by exploiting 3D stacking structure
- Existing 2D side-channel attack (SCA) countermeasures may induce high overhead in 3D scenario
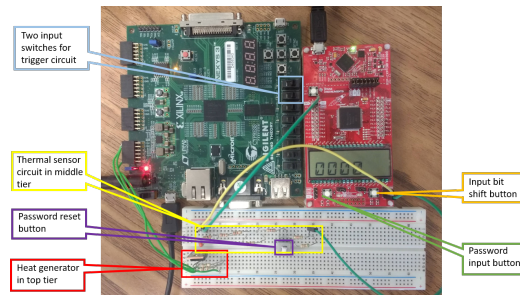
Motivation

- Comprehensive 3D hardware Trojan characterization is needed to inspire hardware security community to generate effective new countermeasures
- Low cost protection mechanisms are desired to better secure 3D ICs from SCA

Key contribution 1: Characterization of Four 3D Trojan cases
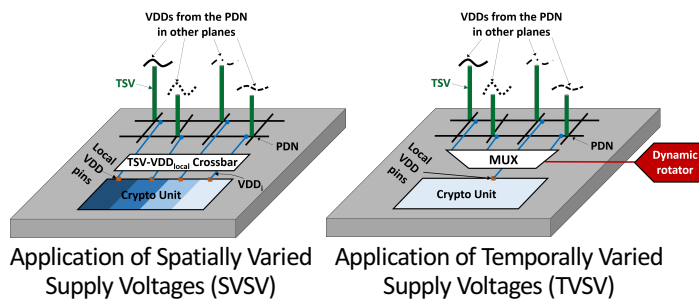
- 3D Trojan characterization
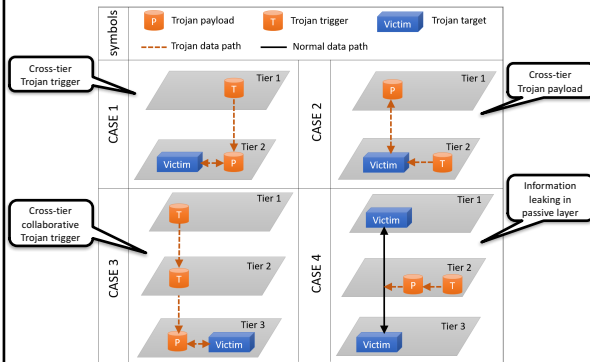
- Trojan hardware demo

- Thermal-triggered Trojan successfully overwrote the password used in an authentication system
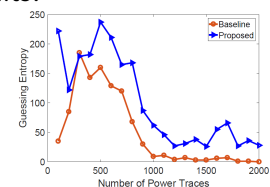
Key contribution 2: Mitigating SCA using 3D internal noise

- 3D power distribution network (PDN) noise is exploited to thwart the correlation power analysis (CPA) attack

Application of Spatially Varied Supply Voltages (SVSV)

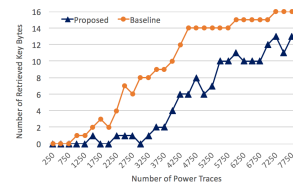Application of Temporally Varied Supply Voltages (TVSV)

- Experimental results:
  - Improved guessing entropy by SVSV
  - Reduced key retrieval speed by TVSV

Conclusion

- Proposed 3D Trojan characterization reveals the potential Trojan threats for 3D ICs
- Proposed PDN noise based countermeasure works as an effective and efficient SCA mitigation for 3D ICs

Impact

- The proposed 3D hardware Trojan characterization enriches existing Trojan models in hardware security community
- 3D ICs facilitate defenders to exploit new resources to thwart side-channel attacks